Jurlind Budurushi, Annika Hilt, Melanie Volkamer

Untersuchung des Sicherheits-bewusstseins im Kontext von "E-Mail made in Germany“

Dieser Artikel erscheint in der Zeitschrift Datenschutz und Datensicherheit.

Das Projekt „E-Mail made in Germany“ wurde als Reaktion auf die Snowden Enthüllungen, insbesondere das grundlose Eindringen in die Privatsphäre von Emailnutzern, initiiert. Das Ziel von „E-Mail made in Germany“ ist es den Emailnutzern in Deutschland einen hohen Sicherheits- und Datenschutzstandard anzubieten. Um Emailnutzer bewusst auf die existierenden Gefahren in Umgang mit E-Mails zu machen, hat „E-Mail made in Germany“ eine breitangelegte Werbekampagne gestartet. Im Mittelpunkt der Kampagne stand ein 30 sekündiger TV Spot. Ziel dieses Artikels ist es den Einfluss dieses TV Spots auf das Sicherheitsbewusstsein von Emailnutzern zu erforschen. Aus diesem Grund wurde eine Laborstudie mit 20 Teilnehmern durchgeführt. In der Studie sollten Teilnehmer an zwei unterschiedlichen Emailkommunikation-Szenarien, vor und nach dem TV Spot, kennzeichnen, ob unbefugte Dritte E-Mails lesen können. Die Ergebnisse der Studie zeigen, dass der TV Spot keinen positiv begründeten Einfluss auf das Sicherheitsbewusstsein der E-Mailnutzer hat. Zusätzlich zeigen die Ergebnisse, dass Emailnutzer nicht auf die üblichen Sicherheitsindikatoren von Webbrowsern achten, um Sicherheitsprobleme zu erkennen. Um diese Situation zu verbessern sollte die Verwendung von Tools wie PassSec+, und Methoden wie bei NoPhish in Betracht gezogen werden.

1 Einleitung

Im Rahmen der Snowden Affäre im Jahr 2013 wurde streng geheime Emailkommunikation zwischen den Geheimdiensten den Vereinigten Staaten und dem Vereinigten Königreich enthüllt [1]. Unter anderem wurden E-Mails von hochrangigen ausländischen Beamten verschiedener Länder und E-Mails von ausländischen Geheimdiensten veröffentlicht [2]. Zahlreiche Dokumente, insbesondere die Dokumente zum Programm PRISM [3] zeigten, dass E-Mails von unbefugten Dritten gelesen werden können und grundlos in die Privatsphäre der Emailnutzer eingedrungen wurde. Als Reaktion auf diese Überwachungs- und Spionageaffäre wurde das Projekt „E-Mail made in Germany“ initiiert. Das Ziel von „E-Mail made in Germany“ besteht darin, einem Großteil der Emailnutzer in Deutschland eine sichere Emailkommunikation ermöglichen zu können. „E-Mail made in Germany“ soll den Emailnutzern einen hohen Sicherheits- und Datenschutzstandard durch eine standardisierte und sichere Kommunikation bieten. Dabei wird die Übertragung der E-Mails zwischen Client-Server und Server-Server verschlüsselt, zusätzlich werden die Daten nur in Deutschland gemäß deutschem Datenschutz verarbeitet und gespeichert.

Um das Sicherheitsbewusstsein von Emailnutzern zu erhöhen beziehungsweise ein sicheres Verhalten im Umgang mit E-Mails zu induzieren, hat „E-Mail made in Germany“ eine breitangelegte Werbekampagne gestartet. Neben Bannern auf diversen Internetseiten steht im Mittelpunkt dieser Werbekampagne ein 30 sekündiger TV Werbespot. Dieser Spot soll einen Anstoß zum sensiblen Umgang mit der persönlichen Kommunikation geben und insbesondere die Botschaft vermitteln, dass niemand will, dass seine Mails mitgelesen werden. Eine repräsentative Untersuchung des Marktforschungsinstituts „YouGov“ zeigt, dass die Mehrheit der Befragten (58%) die Initiative „E-Mail made in Germany“ als "sehr hilfreich [ansehen], weil sie nicht möchten, dass unbefugte Dritte ihre E-Mails mitlesen können“. [1] Im Gegensatz dazu bemängeln Websites wie heise.de oder der Chaoscomputerclub den gerin-

[1] http://www.heise.de/netze/meldung/E-Mail-made-in-Germany-Vollstaendig-umgesetzt-dennoch-unzureichend-2179269.html zuletzt zugegriffen am 29 März 2016

gen Nutzen der Initiative und warnen vor einer „Mogelpackung“.[2] Motiviert durch diese unterschiedlichen Wahrnehmungen und Bewertungen von „E-Mail made in Germany“ soll in diesem Artikels der Einflusses des Werbespots auf das Sicherheitsbewusstsein von Emailnutzern erforscht/dargestellt werden. Hierzu erreichen wurde eine Laborstudie mit 20 Teilnehmern (Emailnutzern) durchgeführt.

Der Rest dieses Artikels ist wie folgt strukturiert: der zweite Abschnitt dient als Hintergrund zu der Initiative, d.h. das Konzept „E-Mail made in Germany“ und der untersuchte Werbespot werden näher erläutert. Abschnitt drei beschreibt die Benutzerstudie und berichtet über die entsprechenden Ergebnisse. Abschließend werden diese Ergebnisse in Abschnitt vier analysiert und diskutiert.

2 Hintergrund: „E-Mail made in Germany“

2.1 Das Konzept

Das Projekt „E-Mail made in Germany“ wurde im August 2013 als Reaktion auf die Überwachungs- und Spionageaffäre 2013 um Edward Snowden initiiert. Gründungsmitglieder sind United Internet mit den Diensten WEB.DE und GMX sowie die Deutsche Telekom mit t-online. Mittlerweile wurde der Dienst auf freenet sowie die beiden größten Hosting Unternehmen Deutschlands STRATO (Deutsche Telekom) sowie 1&1 (United Internet) ausgeweitet. Damit profitieren circa 70% (50 Millionen) der privaten Emailnutzer und 3 drei Mio. gewerblichen Kunden in Deutschland (Freiberufler, kleine und mittlere Unternehmen).[3] Außerdem können alle Unternehmen oder Institutionen mit eigener E-Mail Infrastruktur sich über den TÜV Rheinland für „E-Mail made in Germany“ zertifizieren lassen. Hierdurch soll eine standardisierte Kommunikation zwischen den Unternehmen und Geschäftspartnern möglich sein. „E-Mail made in Germany“ soll laut eigener Aussage den Kunden einen hohen Sicherheits- und Datenschutzstandard bieten, die Kernversprechen lauten wie folgt:

-Verschlüsselung der Server-Server-Übertragung,
-Verschlüsselung der Client-Server-Übertragung.
-Verarbeitung und Speicherung aller Daten nur in Deutschland gemäß deutschem Datenschutz
-Kennzeichnung sicherer E-Mail-Adressen.[4]

Jeglicher Datenaustausch, das heißt sowohl zwischen Endgerät und Emailserver als auch zwischen den einzelnen Emailservern, wird immer SSL-verschlüsselt [4] übermittelt. Hierzu wurden alle Mail Zugänge im „E-Mail made in Germany“-Verbund Anfang 2014 auf SSL-Verschlüsselung umgestellt, seit dem 29. April 2014 wird der gesamte Emailverkehr nach diesen Standards abgewickelt. Außerdem haben alle Partner Perfect Forward Secrecy [5], [6] implementiert (ein weiterer Schutzmechanismus gegen das nachträgliche Entschlüsseln von Daten) und die verwendeten Schlüssel wurden auf Standard AES 256 [7] aufgerüstet. Zusätzlich wurde ein neues Verfahren zur Zertifikatsvalidierung und Identitätsprüfung unter den Providern eingesetzt. Im Mittelpunkt der breitangelegten Werbekampagne stand neben Bannern auf diversen Internetseiten vor allem ein 30 sekündiger TV Spot.

2.2 Der Werbespot

Sketchartig wird immer wieder eine ähnliche Situation gezeigt: eine junge Frau (Schauspielerin Sina-Maria Gerhardt) versucht mehr oder weniger dreist an die E-Mails von Passanten zu gelangen. Mal fragt sie höflich nach, ob sie die E-Mails lesen dürfe, mal versucht sie direkt das Smartphone oder den Laptop einfach zu entreißen. Die Reaktionen darauf sind immer gleich: durchweg Erstaunen und Ablehnung seitens der Passanten, hierbei reichen die Antworten von einem kurzen „nein“ über ein deutliches „Finger weg“ bis zu einem klaren „ich möchte das nicht“. Die Botschaft des Spots wird deutlich kommuniziert: niemand will, dass seine Mails mitgelesen werden. „Der Spot soll hier einen Anstoß zum sensiblen Umgang mit der persönlichen Kommunikation geben und aufzeigen, dass es Alternativen gibt“[5], erklärt Jan Oetjen, Geschäftsführer von GMX und WEB.DE, die Story. Neben dem 30 sekündigen TV Spot existiert eine kürzere Version auf YouTube. Diese hat bereits knapp 8.600 Aufrufe (Stand: 29. März 2016). Ebenso wurden auf diversen Internetseiten Banner geschaltet um eine jüngere Zielgruppe, vor allem Jugendliche und junge Erwachsene zwischen 14 und 29 Jahren[6] anzusprechen und für die Thematik zu sensibilisieren. Die Initiatoren des Spots GMX und WEB.DE (mit der Mediaagentur Mindshare) sowie die deutscher Telekom (mit der Mediaagentur Mediacom) versichern, der Spot sei authentisch und nicht gestellt. „Wir haben extra ein sehr anschauliches Format gewählt, um die Nutzer für das Thema Datenschutz zu sensibilisieren und sich am Ende ganz bewusst für einen Provider zu entscheiden, dem sie ihr persönliches Postfach anvertrauen wollen.“[7] (so Jan Oetjen, Geschäftsführer von GMX und WEB.DE). Das Konzept stammt von der renommierten Werbeagentur Jung von Matt, insgesamt wurde ein zweistelliger Millionenbetrag in die Kampagne investiert. Laut GMX konnte durch die Kampagne der Bekanntheitsgrad des Konzepts „E-Mail made in Germany“ von 32 Prozent auf 65 Prozent bei GMX Nutzern gesteigert werden.[8]

3 Benutzerstudie

3.1 Ziel

Das Ziel dieser Benutzerstudie besteht in der Erforschung des Einflusses des Werbespots von „E-Mail made in Germa-

[2] http://ccc.de/de/updates/2013/bullshit-made-in-germany zuletzt zugegriffen am 29 März 2016

[3] http://www.e-mail-made-in-germany.de/img/presse/download/29042014_Praesentation_E-Mail-made-in-Germany.pdf zuletzt zugegriffen am 29 März 2016

[4] http://www.e-mail-made-in-germany.de/img/presse/download/29042014_Praesentation_E-Mail-made-in-Germany.pdf, Seite 2 zuletzt zugegriffen am 29 März 2016

[5] http://newsroom.gmx.net/2014/04/29/neuer-tv-spot-niemand-will-dass-seine-mails-mitgelesen-werden/ zuletzt zugegriffen am 29 März 2016

[6] http://www.goldmedia.com/newsletter/presseverteiler/pressemeldung-26022015-youtube-wird-alltagsmedium/ zuletzt zugegriffen am 29 März 2016

[7] http://newsroom.web.de/2014/09/08/neuer-tv-spot-wirbt-fuer-e-mail-made-in-germany/ zuletzt zugegriffen am 29 März 2016

[8] http://newsroom.gmx.net/2015/01/01/10-jahre-die-gedanken-sind-frei-gmx-wirbt-zum-jubilaeum-mit-neuauflage-des-spots/ zuletzt zugegriffen am 29 März 2016

ny“ auf das Sicherheitsbewusstsein von Emailnutzern. Dazu wurde eine Laborstudie mit 20 zufällig ausgewählten Teilnehmern (Emailnutzern) durchgeführt. Im Folgenden beschreiben wir das Design und den Ablauf der Studie. Zusätzlich berichten wir über die Stichprobe und die Ergebnisse der Studie.

3.2 Design

Die Benutzerstudie war eine Laborstudie, in der die Teilnehmer zu einem bestimmten Ort und Raum eingeladen waren, um an der Studie teilzunehmen. Hierbei wurden 20 Teilnehmer aus dem registrierten Teilnehmer-Pool zufällig für die Studie ausgewählt und in einer zufälligen Reihenfolge eingeladen. Die für die Studie benötigten Materialien wurden von dem Versuchsleiter zur Verfügung gestellt.

Die Studie bestand aus drei Phasen. In der ersten Phase wurden die Teilnehmer mit zwei unterschiedlichen Szenarien der Emailkommunikation nacheinander konfrontiert. Um den Teilnehmern den Emailaustausch greifbarer zu machen, wurde die Emailkommunikation in sieben abstrakte Schritten (Positionen) unterteilt: 1) Rechner des Absenders 2) Kommunikation zwischen dem Rechner des Absenders und des jeweiligen E-Mail Servers 3) E-Mail Server des Absenders 4) Kommunikation zwischen dem E-Mail Server des Absenders und dem E-Mail Server des Empfängers 5) E-Mail Server des Empfängers 6) Kommunikation zwischen dem Rechner des Empfängers und des jeweiligen E-Mail Servers und 7) Rechner des Empfängers. Die Aufgabe der Teilnehmer in der ersten Phase bestand darin, anzugeben, ob Dritte unbefugten Zugriff auf versandte E-Mails in den jeweiligen sieben Schritten haben. Es ist wichtig zu beachten, dass in der Studie die Annahme getroffen wurde, dass wenn Verbindungen zwischen zwei Rechnern mit dem allgemein bekannten SSL Protokoll gesichert sind, kein unbefugter Zugriff durch Dritte möglich ist. Dies wurde den Teilnehmern auch so mitgeteilt. In der zweiten Phase sahen die Teilnehmer den Werbespot von „E-Mail made in Germany“. Danach, in der dritten Phase, bestand die Aufgabe der Teilnehmer wieder darin die Szenarien zu bewerten, d.h. ob Dritte unbefugten Zugriff auf versandte E-Mails an den jeweiligen sieben Schritten haben.

Um den Einfluss des Werbespots auf das Sicherheitsbewusstsein von den Teilnehmern zu messen, wurden folgende zwei Szenarien mit unterschiedlichen Schwerpunkten ausgewählt: 1) GMX an Telekom; und 2) GMX an Google. Das erste Szenario dient dazu herauszufinden, ob Teilnehmer ein mögliches Sicherheitsproblem (konkret: dass der Anmeldebereich bei GMX, im Gegensatz zu Telekom, nicht mit dem SSL Protokoll gesichert ist) erkennen können, obwohl GMX selbst an dieser Stelle widersprüchlicherweise für mehr Sicherheitsbewusstsein mit dem Werbespot wirbt. Mithilfe des zweiten Szenarios soll untersucht werden, ob Teilnehmer ein weiteres Sicherheitsproblem, nämlich, dass die Verbindung zwischen den E-Mail Servern von zwei unterschiedlichen Providern nicht als gesichert angenommen werden kann, erkennen können.

3.3 Ablauf

In der Studie durchliefen die Teilnehmer die folgenden Schritte:

1. Die Teilnehmer lasen und unterschrieben die Einwilligungserklärung zur Teilnahme an der Studie.
2. Die Teilnehmer machten sich mit dem Ziel der Studie vertraut.
3. Die Teilnehmer schätzten ihre Kenntnisse zum Thema Emailsicherheit auf einer Skala von sehr wenig bis sehr hoch ein.
4. Die Teilnehmer wurden anhand eines allgemeinen Szenarios, welches den Austausch von E-Mails zwischen zwei Emailnutzern in sieben abstrakten Schritten (Positionen) beschreibt, mit der Emailkommunikation vertraut gemacht. Siehe Abbildung 1.

Abbildung 1: Allgemeines Szenario zur Emailkommunikation.

5. Den Teilnehmern wurde durch das allgemeine Szenario, dargestellt in Abbildung 1, ihre Aufgabe erläutert. Dabei sollten sie auf jedem der sieben verschiedenen Schritte der Emailkommunikation kennzeichnen, ob versandte E-Mails von Dritten, Empfänger und Absender ausgeschlossen, gelesen werden können. Hierbei konnten die Teilnehmer drei unterschiedliche Kennzeichnungen verwenden, die in der Tabelle 1 beschrieben werden.

Nummer	Fall	Kennzeichnung
1	Dritte können versandte E-Mails nicht lesen.	✕
2	Dritte können versandte E-Mails lesen.	√
3	Nicht sicher, ob Dritte versandte E-Mails lesen können.	?

Tabelle 1: Beschreibung der unterschiedlichen Kennzeichnungen.

6. Den Teilnehmern wurden die zwei unterschiedlichen Szenarien, siehe Abbildung 2 und 3, zur Emailkommunikation nacheinander angezeigt. Dabei sollten Teilnehmer jedes Szenario, entsprechend der Erklärung in Schritt 6, kennzeichnen. Neben dem Szenario selbst wurden den Teilnehmern auch Bilder des Anmeldebereichs und des Posteingangs der im Szenario beteiligten Kommunikationspartner, z.B. GMX und Telekom, gezeigt.

Abbildung 2: Erstes Szenario: E-Mail von GMX an Telekom versandt.

Abbildung 3: Zweites Szenario: E-Mail von GMX an Google versandt.

7. Die Teilnehmer wurden gefragt, ob sie das Konzept „E-Mail made in Germany“ kennen.

8. Den Teilnehmern wurde der Werbespot von „E-Mail made in Germany“ angezeigt.
9. Die Teilnehmer wurden gebeten die zwei unterschiedlichen Szenarien wieder zu kennzeichnen.
10. Die Teilnehmer füllten den Fragebogen zur Person aus.

3.4 Stichprobe

Die Teilnehmer wurden aus dem Campus der Technischen Universität Darmstadt rekrutiert. Insgesamt nahmen 20 Teilnehmer (3 weiblich, 17 männlich) im Alter von 20 bis 36 Jahre an der Studie teil. Die Altersverteilung und der Bildungsstand der Teilnehmer sind in den Tabellen 2 und 3 dargestellt. Zusätzlich stellt Tabelle 4 die Einschätzung der Teilnehmer bezüglich ihrer Kenntnisse zum Thema Emailsicherheit dar.

Alter	**Anzahl der Teilnehmer N=20**
22	2
24	1
25	3
26	2
27	3
28	2
29	4
31	2
36	1

Tabelle 2: Altersverteilung der Teilnehmer.

Bildungsstand	**Anzahl der Teilnehmer N=20**
Ausbildung	1
Bachelor	15
Master	2
Ph.D.	2

Tabelle 3: Bildungsstand der Teilnehmer

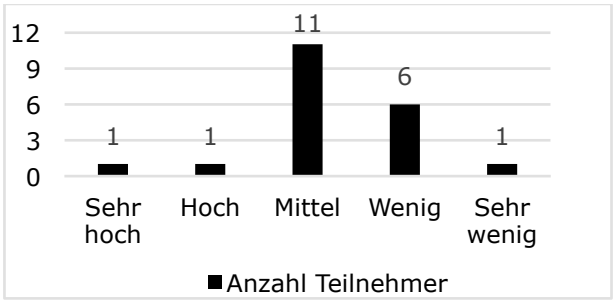

Abbildung 4: Kenntnisse der Teilnehmer bezüglich des Themas Emailsicherheit.

3.5 Ergebnisse

Die Ergebnisse der Studie sind in den Tabellen 4 bis 7 entsprechend dem jeweiligen Szenario dargestellt.

Position und Korrekte Antwort	**Anzahl der Teilnehmerantworten nach Kennzeichnungen**		
	√	×	?
1: √	12	4	4
2: ×	10	3	7
3: √	14	1	5
4: ×	11	3	6
5: √	9	4	7
6: ×	9	4	7
7: √	12	4	4

Tabelle 4: Erstes Szenario (GMX ↔ Telekom), vor dem Werbespot.

Position und Korrekte Antwort	**Anzahl der Teilnehmerantworten nach Kennzeichnungen**		
	√	×	?
1: √	10	5	5
2: ×	7	7	6
3: √	10	8	2
4: ×	5	10	5
5: √	9	8	3
6: ×	6	8	6
7: √	10	5	5

Tabelle 5: Erstes Szenario (GMX ↔ Telekom), nach dem Werbespot.

Position und Korrekte Antwort	Anzahl der Teilnehmerantworten nach Kennzeichnungen		
	√	×	?
1: √	11	4	5
2: ×	9	2	9
3: √	13	3	4
4: √	13	1	6
5: √	15	2	3
6: ×	11	2	7
7: √	12	3	5

Tabelle 6: Zweites Szenario (GMX ↔ Google), vor dem Werbespot.

Position und Korrekte Antwort	Anzahl der Teilnehmerantworten nach Kennzeichnungen		
	√	×	?
1: √	10	5	5
2: ×	8	8	4
3: √	9	10	1
4: √	12	4	4
5: √	14	1	5
6: ×	14	3	4
7: √	12	2	6

Tabelle 7: Zweites Szenario (GMX ↔ Google), nach dem Werbespot.

Diskussion

Nach der Analyse der von den Teilnehmern angegebenen Antworten und Kennzeichnungen, zeigen die Ergebnisse, dass Emailnutzer nicht immer wissen, an welcher Stelle E-Mails von unbefugten Dritten gelesen werden können. Dies lässt sich auch durch die Gegenüberstellung der Kennzeichnungen beim ersten und zweiten Szenario bestätigen. Der Vergleich zeigt, dass Emailnutzer die Verbindung zwischen den E-Mail Servern von zwei unterschiedlichen Providern nicht als ungesichert annehmen. Diese Situation wird auch durch den Werbespot nicht verbessert, es bestätigt sich lediglich der Vorwurf des Chaoscomputerclubs: „den Nutzern der E-Mail-Dienste [wird] jedoch vorenthalten, dass eine Verschlüsselung der Verbindung zwischen den Anbietern noch nicht bedeutet, dass die E-Mails dort auch verschlüsselt abgelegt werden. […] Der Anbieter und befreundete Geheimdienste haben nach wie vor vollen Zugriff auf die Inhalte der E-Mails und können diese somit auch vollständig auswerten“.

Zusätzlich zeigen die Ergebnisse des ersten Szenarios, dass Emailnutzer nicht auf die üblichen Sicherheitsindikatoren von Webbrowsern achten, um Sicherheitsprobleme zu erkennen. Um das Sicherheitsbewusstsein beziehungsweise –verhalten bezüglich der Erkennung von Sicherheitsproblemen zu verbessern, sollten Tools wie PassSec+ [8] in Betracht gezogen werden.

Nichtsdestotrotz zeigen die Ergebnisse, dass die Anzahl korrekter Kennzeichnungen nach dem Spot im Allgemeinen anstieg. Die Ergebnisse deuten aber auch an, dass der Spot keinen positiv begründeten Einfluss auf das Sicherheitsbewusstsein der E-Mailnutzer hat. Während die Anzahl korrekter Kennzeichnungen bei den Absender/Empfänger Rechner und E-Mail Server sank, stieg die Anzahl korrekter Kennzeichnungen bei der Kommunikationsverbindungen. Diese Erkenntnisse lassen sich auch durch das zweite Szenario im Vergleich zu dem ersten Szenario bestätigen. Um einen positiv begründeten Einfluss auf das Sicherheitsbewusstsein von Emailnutzern zu erzielen, sollten Methoden aus anderen Kontexten, zum Beispiel die Methoden von NoPhish [9] im Kontext von Phishing, in Betracht gezogen werden.

Literatur

[1] Luke Harding. The Snowden Files: The Inside Story of the World’s Most Wanted Man. Vintage, New York City, 2014.

[2] Barton Gellman Ellen Nakashima. Court gave nsa broad leeway in surveillance, documents show, 2014. Zuletzt gesehen, März 29, 2016, http://www.washingtonpost.com/world/national-security/court-gave-nsa-broad-leeway-in-surveillance-documents-show/2014/06/30/32b872ec-fae4-11e3-8176-f2c941cf35f1_story.html

[3] Luke Harding. Edward Snowden: Geschichte einer Weltaffäre. C.W. Leske Verlag, Pfalzstr. 12, 40477 Düsseldorf, Germany, 2014.

[4] Rolf Oppliger. Ssl and tls: Theory and practice (artech house information security and privacy). Artech House Inc., ISBN-13:978-1596934474.

[5] Krawczyk, Hugo. "Perfect forward secrecy." Encyclopedia of Cryptography and Security. Springer US, 2005. 457-458.

[6] Sun, Hung-Min, Bin-Tsan Hsieh, and Hsin-Jia Hwang."Secure e-mail protocols providing perfect forward secrecy. “Communications Letters, IEEE 9.1 (2005): 58-60.

[7] http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, zuletzt gesehen, März 29, 2016.

[8] SECUSO, Fachbereich Informatik, TU-Darmstadt. PassSec+ - ein add-on das ihre passwörter, zahlungsdaten und privatsphäre schützt, 2015.Retrieved May 28, 2015, from https://www.secuso.informatik.tu-darmstadt.de/de/research/results/passsec-deutsch/.

[9] Canova, G., Volkamer, M., Bergmann, C., Borza, R., Reinheimer, B.,Stockhardt, S., & Tenberg, R. (2015). Learn to Spot Phishing URLs with the Android NoPhish App. In Information Security Education Across the Curriculum (pp. 87-100). Springer International Publishing.